CHAPTER 2

UMCS NETWORK ARCHITECTURE

2-1 TWO-TIERED ARCHITECTURE

2-1.1 General.

As shown in Figure 2-1 the basewide network consists of a two-tiered architecture consisting of a building-level network with a building point of connection (BPOC) that provides an interface to the UMCS. Generally, the UMCS will be a basewide system, but may initially consist of only one (or few) building-level networks with the capability of being expanded to include additional buildings.

2-1.2 Building-Level Network.

As described in UFC 3-410-02, a low-speed communications network is used to interconnect the building-level LonWorks direct digital control (DDC) nodes, also referred to as devices and controllers. This building-level network speed will usually be 78.1 Kbps. In some cases a higher speed 1.25 Mbps backbone may be used with lower speed 78.1 Kbps segments connected to this backbone. The building-level network is an open communications protocol network and can be extended by third party contractors. Variations to this basic architecture are possible:

- Multiple buildings can share a common building-level network. For example, two or more adjacent buildings can be physically linked by a common network cable as long as network restrictions described in UFC 3-410-02 and UFGS-15951 are adhered to such as cable length and the total number of nodes. In this case, a single BPOC can be used to connect these buildings to the UMCS.

- A large building can have multiple building-level ANSI-709.1 Networks. In this case, the building-level contractor will install multiple independent building-level networks and the UMCS contractor will install a separate BPOC for each network.

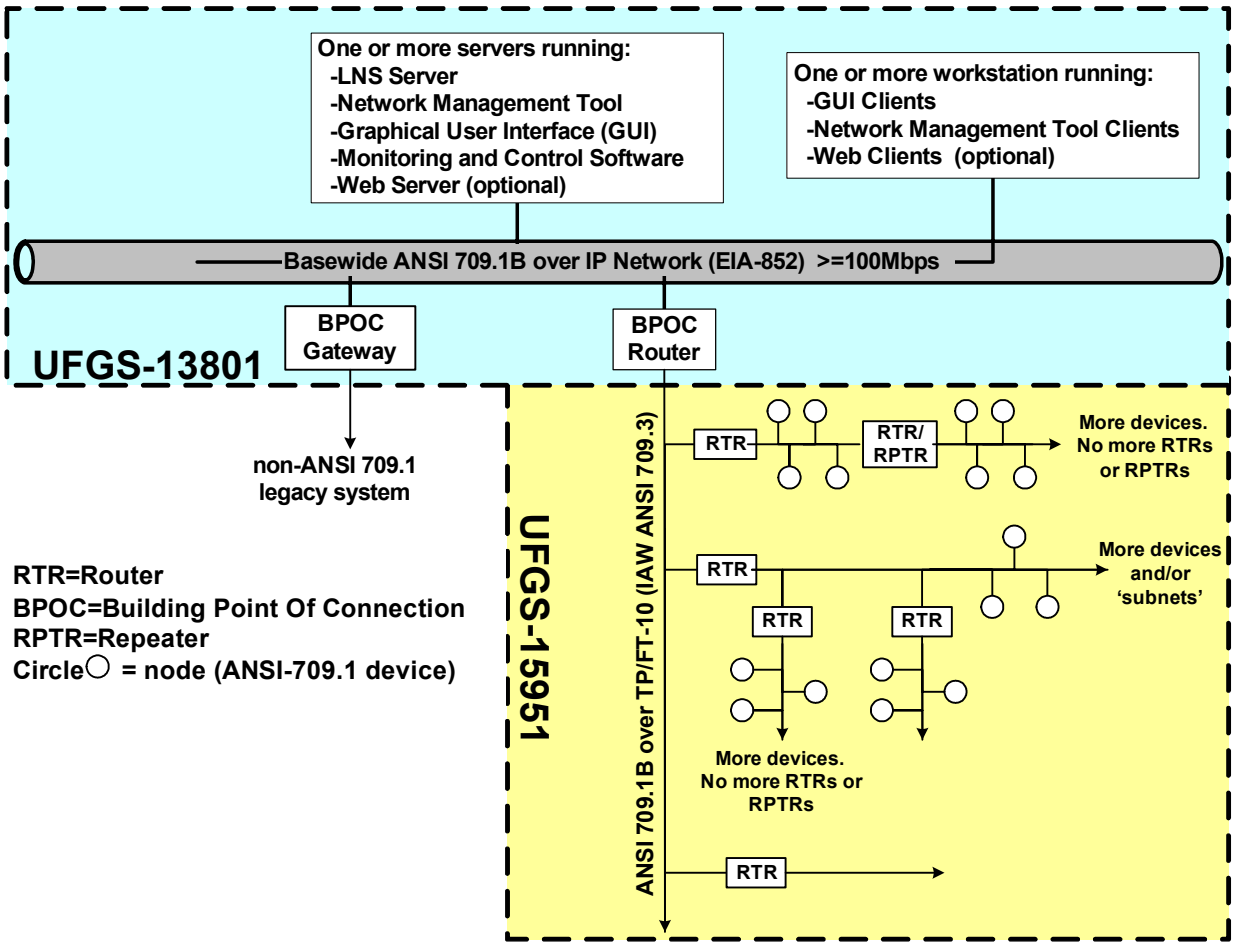

Figure 2-1. UMCS Basic Architecture

2-1.3 **Basewide UMCS Network.**

At the UMCS level, the building point of connection (BPOC) interfaces the building-level network to high-speed Internet Protocol (IP) in support of inter-building communication and also serves as the communications link between the building-level controls and the UMCS personal computer (PC) server and workstations.

2-2 **BUILDING POINT OF CONNECTION (BPOC)**

The BPOC is the demarcation point between the UMCS and the building-level network. It defines the division of responsibility between the UMCS contractor and the building-level control system contractor. The contractual responsibilities of the UMCS contractor and the building-level contractor will be project-specific, but in general the building-level contractor is responsible for installing the building-level network and LonWorks controls while the UMCS contractor is responsible for connecting the building-level network to the UMCS. The BPOC must be a LonWorks router, or in the case of an interface to a legacy (existing) system, it could be a Gateway. In each of these cases, the BPOC is installed and configured per the requirements defined in UFGS-13801.

2-2.1.1 **BPOC Router.**

The preferred building point of connection is an ANSI 709.1 TP/FT-10 to IP Router which converts building-level communication protocol to EIA-852 (ANSI 709.1 tunneled over IP), and vice versa. The BPOC performs layer 3 routing of ANSI 709.1 packets over an Ethernet network in accordance with IEEE 802.3. The BPOC router supports two basic functions:

- It manages communications traffic by routing designated standard network variable types (SNVTs) between different local building-level networks and the UMCS Servers/Workstations.

- It permits UMCS Servers/Workstation access to individual nodes/controllers in support of network and device configuration using an LNS compatible network tool.

2-2.1.2 **BPOC Gateway.**

The sole function of a BPOC Gateway is to convert proprietary vendor-specific non-ANSI 709.1 building-level protocol data to ANSI 709.1 as SNVTs, and vice versa. Gateways are used to support legacy (existing) building-level DDC systems. Gateways are not intended to serve as an interface in new-project DDC systems, unless specifically approved by the government design authority or MCX. A Gateway is sometimes referred to as a communications Bridge.

2-2.1.3 **Other BPOCs.**

Other BPOCs are prohibited unless specifically approved by the design authority (District or MCX).

2-3 **BASEWIDE INTERNET PROTOCOL (IP) NETWORK.**

The basewide UMCS network will be based on Internet Protocol (IP) Ethernet standard IEEE 802.3. This network will support the data transmission requirements of the UMCS including initial setup and configuration of the network devices along with post-setup day-to-day intercommunication of all network devices (UMCS servers, workstations, BPOCs, and building-level controllers/nodes). It is important to note that a properly designed UMCS Network will require minimal network bandwidth compared to many Information Technology (IT) applications and compared to the available bandwidth on a modern basewide IT backbone. Use of the IP network will need to be coordinated with the Directorate Of Information Management (DOIM) as described in the IP Networking and Implementation chapters. The intent of this coordination is to address network management and security issues. Related design issues and details are described elsewhere in this document.

2-4 **UMCS SERVERS AND WORKSTATIONS.**

2-4.1 **General.**

The UMCS front-end hardware and software consists of a number of distinct logical functional blocks, as shown in Figure 2-2. It is based on LonWorks Network Services (LNS) network operating system. LNS provides an infrastructure for network tools and UMCS applications helping to ensure interoperability of these tools and applications by providing open data access services for HMI (Human-Machine Interface) and SCADA

(Supervisory Control And Data Acquisition) applications as well as remote access via LonWorks or IP networks. The client-server architecture allows multiple clients to access the LNS database simultaneously, thereby permitting access by multiple operators/users from multiple workstations as well as multiple system integrators/contractors during network and device configuration.

Figure 2-2. UMCS client-server architecture

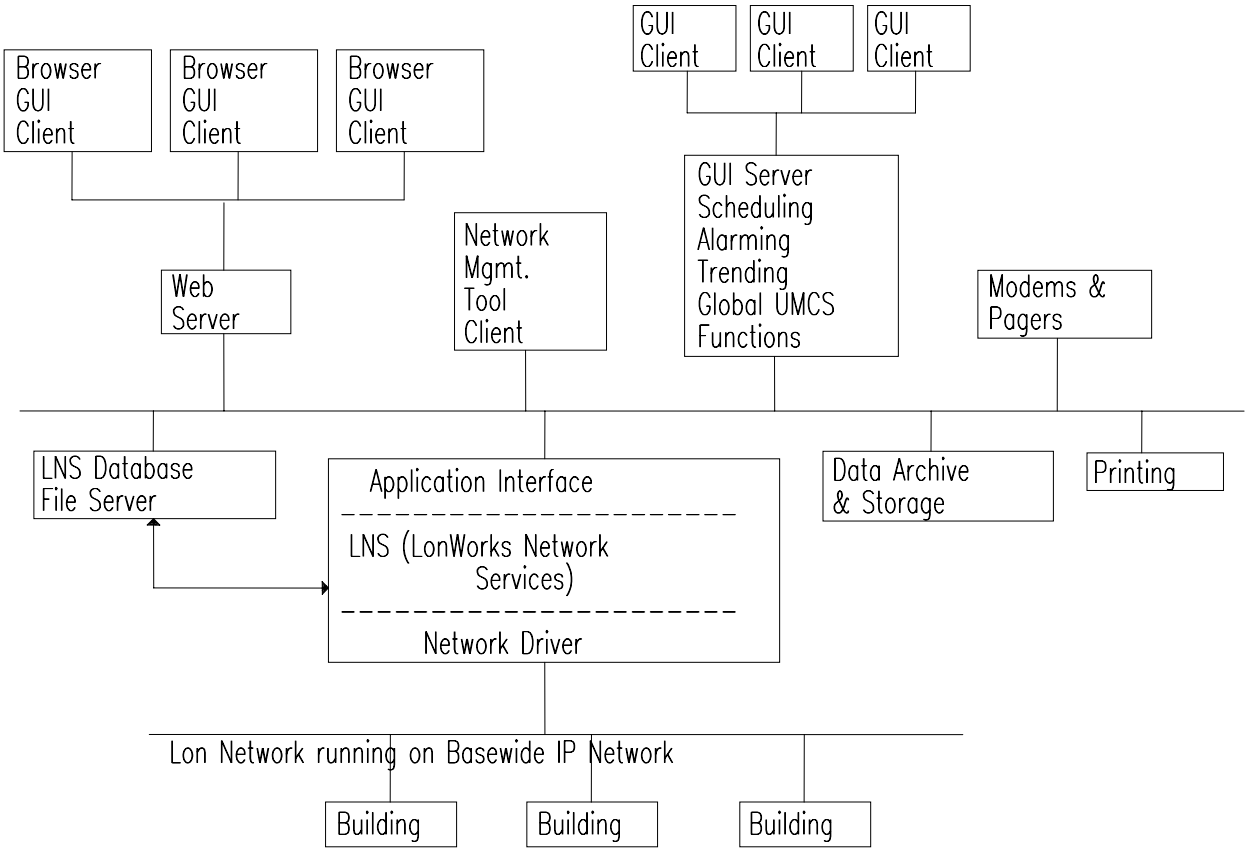

Figure 3-2: UMCS Client-Server Architecture

2-4.2 **LNS Server.**

The LNS server provides network management. It manages the Network and interfaces higher level components to the building-level control network through the basewide UMCS network. It contains an application interface to coordinate access to the LNS database file server and a network driver to coordinate access to the IP network.

2-4.3 **LNS Database File Server.**

The LNS database resides on a file server. The LNS Database stores an ‘image’ of the network configuration/definitions for all LonWorks nodes including the standard network variable types (SNVTs). For a very large installation, in excess of 32,000 nodes, multiple LNS databases may be required. The LNS database file server is an integral

part of LNS, but it may reside on hardware separate from the LNS Server such as a separate file server.

2-4.4 **Network Management Tool Client.**

A Network Management Tool Client is a software package that serves as a user interface to the LNS server. This tool will likely reside on the same hardware as the LNS server, but may also be run from other computers anywhere on the IP network, or, with the proper hardware interface, from a building-level network.

2-4.5 **GUI Server.**

The graphical user interface (GUI) server, sometimes referred to as a UMCS workstation (server), manages, stores, and executes UMCS applications and operations such as scheduling, alarming, trending, and other global functions. These functions are logically distinct, but are ordinarily contained in a single software package. This software package interacts with the Application Interface in the LNS server, but may reside on a computer separate from the LNS server.

2-4.6 **GUI Client.**

A GUI client is a client of the GUI server in the client-server architecture. It has a graphical user interface and functions as an operator workstation to allow user/operator access to the GUI server as it performs UMCS workstation-type functions. Depending on the software vendor, the GUI client may be inseparable from the GUI Server where one software package includes both. In this case multiple GUIs requires the purchase of multiple GUI server packages. Other vendors offer GUI clients at reduced cost (sometimes via a licensing arrangement) where one GUI server package can support multiple GUI clients running on other computers. GUI clients typically require that vendor-specific software be loaded on the GUI client computer. This software is sometimes referred to as thick-client software.

2-4.7 **Web Server.**

A web server serves up web pages via the Internet to browser-based GUI clients, but not all UMCS vendors provide these web services. Where a web server is used, it must interact with the Application Interface in the LNS server to access network data. The web server may reside on the same machine as the LNS server, but more likely is located on one or more separate PCs.

2-4.8 **Browser GUI Client.**

A browser-based GUI client provides web-based Internet access to web pages served up by a Web Server. These (thin) clients perform the same function as GUI clients but rely only on established Internet browser technologies such as Netscape and Internet Explorer. Unlike a GUI client, a browser client ordinarily does not require vendor-specific (thick client) software on the computer receiving the web pages.

2-4.9 **Modems And Pagers.**

A modem permits remote access to the UMCS. A variety of functions are possible via this dial-up link, but its primary function is to generate alphanumeric pages, typically to send specified critical alarms. In some cases, modems and pagers for critical alarms may reside in and be generated at the building-level on the network.

2-4.10 **Data Archive And Storage.**

The front end system provides long-term storage of programs and data largely in support of the GUI server functions.

2-4.11 **Printing.**

The front end system supports printing services including one or more ink jet, laser, and possibly color printers. For line-by-line printing of alarms, a dot-matrix can be used.

2-4.12 **Computer Hardware Requirements**

The specification gives several minimum requirements for hardware for both computer servers and computer workstations. Many of these requirements are dependent on the application to be run on the server. The reason for this is the rapid advancement in computer hardware and the corresponding increase in software requirements. Rather than give a requirement that would quickly become obsolete (for example "CPU shall be at least 1 GHz Pentium III or equivalent") or excessive for the application, the requirements are based on the stated requirements of the software to be installed. For example one of the popular network configuration tools has a requirement of a 200 MHz Pentium and 128 MB of RAM; a computer purchased to run this software would need to have at least a 500 MHz (250% of 200 MHz) CPU and 384 MB (250% of 128 MB) of RAM.

2-4.12.1 **Server Hardware**

The UMCS is dependent on the operation of several server processes; in particular servers related to the LNS server (possibly including a remote file server for the database) are needed for the UMCS to function. (Note that loss of the UMCS will not prevent the building-level controls from continuing to function in stand-alone mode.) For this reason, UFGS-13801 places specific requirements on hardware that may be used for a computer server.

RAID (Redundant Array of Inexpensive Disks) is a commonly used computer technology for protecting data against disk drive hardware failure. A computer running either a RAID-1 or RAID-5 array (there are other RAID levels which offer this functionality, but RAID-1 and RAID-5 are the most common) will be able to continue uninterrupted operation even after the catastrophic failure of one of the disk drives. (After a drive has failed, the computer should be shut down and the defective drive replaced soon; until the drive is replaced, the data is vulnerable to an additional drive failure.)

Redundant power supplies are another commonly used computer technology to guard against computer hardware failure. The computer is designed with 2 (or more) power supplies; any one of the supplies is sufficient to operate the computer. In case of a power supply failure, the computer will continue to operate on the remaining supply(s). In addition, the hot swap capability means the defective supply can be replaced without shutting the server down.

The DOIM is an excellent source of information on these and other computer hardware technologies that may be used to increase the reliability of computer server hardware.

2-4.12.2 **Workstation Hardware**

Since the UMCS is not dependent on the availability of clients to carry out its key operational functions, there are no additional requirements for computer hardware beyond what is typically procured for a standard desktop computer.